

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平11-7241

(43) 公開日 平成11年(1999) 1月12日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 0 9 C 5/00

G 0 9 C 5/00

G 0 6 F 12/14

3 1 0

G 0 6 F 12/14

3 1 0 Z

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 G

H 0 4 N 7/08

H 0 4 N 7/08

Z

7/081

審査請求 未請求 請求項の数10 F D (全 13 頁)

(21) 出願番号

特願平9-173168

(22) 出願日

平成9年(1997) 6月13日

(71) 出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72) 発明者 斉藤 誠

東京都千代田区丸の内2丁目6番3号 三

菱商事株式会社内

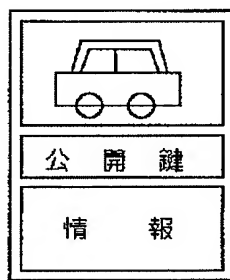
(74) 代理人 弁理士 南條 眞一郎

(54) 【発明の名称】 電子透かしを利用するデジタルコンテンツ管理システム

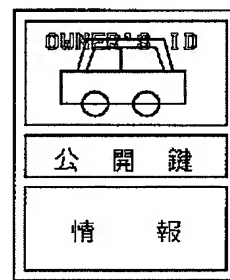
(57) 【要約】

【課題】 デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提供する。

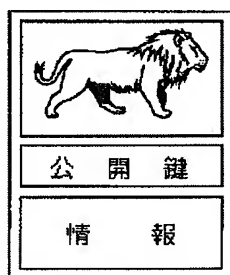
【解決手段】 デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、ネットワークあるいはデータ放送を利用して、デジタルコンテンツ管理プログラムとリンクする監視プログラムあるいは監視コマンドをユーザ装置に送信し、デジタルコンテンツの不正利用を監視する。不正利用されたデジタルコンテンツには可視透かしが埋め込まれ、以後の利用を抑制する。なお、正規の利用であっても不可視の透かしを埋め込むことにより複写・転送等の経路を確認することが可能になる。また、公開鍵を公開鍵配布画面に記入してネットワークあるいは放送により配布する。公開鍵配布画面には公開鍵所有者あるいは利用者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されており、この電子透かしにより公開鍵あるいは利用者の正当性を確認する。



(a)



(b)



(c)



(d)

**【特許請求の範囲】**

【請求項 1】 著作権主張がなされたデジタルコンテンツの管理を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、デジタルコンテンツ管理プログラムがユーザの装置のオペレーティングシステム中にマイクロカーネルとして組み込まれており；前記デジタルコンテンツ管理プログラムとリンクする利用監視プログラムが放送によって前記ユーザ装置に転送され；前記デジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして前記利用監視プログラムが前記デジタルコンテンツの利用状況を監視する。

【請求項 2】 前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を可視透かしとして埋め込む、請求項 1 記載のデジタルコンテンツ管理システム。

【請求項 3】 前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項 1 記載のデジタルコンテンツ管理システム。

【請求項 4】 前記利用状況として保存・複製及び／又は転送が検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項 1 記載のデジタルコンテンツ管理システム。

【請求項 5】 公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、前記公開鍵が公開鍵配布画面に記入されて放送によって配布され；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより公開鍵所有者を確認する。

【請求項 6】 前記公開鍵の所有者の情報として前記公開鍵の所有者の情報の電子指紋が利用される、請求項 5 記載のデジタルコンテンツ管理システム。

【請求項 7】 公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、前記ユーザが前記公開鍵管理センタに前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記公開鍵の

所有者を確認する。

【請求項 8】 前記公開鍵の所有者の情報の代わりに、前記公開鍵の所有者の情報の電子指紋が利用される、請求項 7 記載のデジタルコンテンツ管理システム。

【請求項 9】 公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、前記ユーザが前記公開鍵管理センタに前記ユーザの情報を提示して前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記ユーザの情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離し、前記公開鍵を用いて暗号化されたデジタルコンテンツとともに前記公開鍵配布画面を前記公開鍵の所有者に転送し；前記公開鍵の所有者が前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記ユーザを確認する。

【請求項 10】 前記ユーザに代えて、前記ユーザの情報の電子指紋が利用される、請求項 9 記載のデジタルコンテンツ管理システム。

**【発明の詳細な説明】****【0001】**

【利用分野】本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うシステムに関する。

**【0002】**

【従来の技術】情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができ情報が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム 2 値データであり、自然画及び動画のような情報量が格段に多いデータを扱うことができなかった。

【0003】ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた 2 値データ以外の画像信号もデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【0004】従来広く普及しているアナログコンテンツは保存、複製、加工、転送をする毎に品質が劣化するた

めに、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存、複写、加工、転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルコンテンツの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0005】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデジタルコンテンツを保存、複写、加工することによって有効活用し、加工したデジタルコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオフラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログコンテンツである音声データ及び画像データがデジタルコンテンツ化されてデータベースとされる。

【0006】このような状況において、データベース化されたデジタルコンテンツの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の2次利用について完成された著作権管理手段はない。なお、広告付きソフトあるいはフリーウェアと呼ばれるデジタルコンテンツは利用において原則として使用料を必要としないが、著作権は存在しており、利用の仕方によっては著作権上の制限を受ける場合がある。

【0007】このような状況に鑑みて、本発明者はこれまでにデジタルコンテンツの著作権を保護することを目的としてこれまでに様々な提案を行ってきた。本発明者らは特開平6-46419号及び特開平6-141004号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平6-132916号でそのための装置を提案した。

【0008】また、特開平7-271865号及び特開平8-185448号において、デジタルコンテンツの著作権を管理するシステムについて提案した。これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理センタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【0009】特開平7-271865号に記載されたシステムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む）、保存、複写、加工、転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0010】また、この特開平7-271865号には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存、コピー、転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【0011】本出願が関連する特開平8-287014号において著作権管理を行うためのボード、PCMCIAカードあるいはICカードの形態を有する復号/再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

【0012】特開平8-272745号において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵方式と公開鍵方式を組み合わせることで加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

【0013】特開平8-288940号において、データベース、ビデオオンデマンド（VOD）システムあるいは電子商取引に著作権管理システムを適用するための様々の形態を提案した。

【0014】特開平8-329011号において、複数データを利用・加工する場合の原データ及び新データの著作権保護を第三の暗号鍵及び著作権ラベルを用いて行うシステムを提案した。

【0015】以上説明した本発明者が提案してきたデータ著作権管理システム及びデータ著作権管理装置から理解されるように、データ著作権の管理は著作権管理プログラムによって暗号化/復号化/再暗号化及び利用内容の制限を行うことによって実現される。この暗号技術及び利用制限はコンピュータを使用することによって実現される。

【0016】さらに、ネットワークを経由して秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止すること

が、USP 5 5 0 4 8 1 8, 5 5 1 5 4 4 1 に述べられており、その場合に複数の暗号鍵を用いることが USP 5 5 0 4 8 1 6, 5 3 5 3 3 5 1, 5 4 7 5 7 5 7 及び 5 3 8 1 4 8 0 に述べられており、再暗号化を行うことが USP 5 4 7 9 5 1 4 に述べられている。

【0017】コンピュータを効率的に使用するために、コンピュータの全体の動作を統括するオペレーティングシステム（OS）が用いられている。パーソナルコンピュータ等で使用されている従来のオペレーティングシステムはメモリ管理、タスク管理、割り込み、プロセス間通信という基本的なサービスを扱うカーネル（Kernel）と、その他のサービスを扱うオペレーティングシステムサービスで構成されていた。

【0018】しかしながら、マイクロプロセッサの能力向上、主記憶装置として使用される RAM 価格の低下というコンピュータ側の情勢変化と、コンピュータに対する利用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシステムの規模が肥大している。

【0019】このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

【0020】このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中枢サブシステムとをユーザに依存する部分であるサブシステム（Sub system）として取り除き、ハードウェアの相異を吸収する HAL（Hardware abstraction Layer）、スケジューリング機能、割り込み機能、I/O 管理機能等の基本的部分をマイクロカーネル（Micro kernel）とし、サブシステムとマイクロカーネルの間にシステムサービス API（Application Programming Interface）を介在させてオペレーティングシステムを構成している。

【0021】このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

【0022】コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベデッド（組み込み）用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用

のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリアルタイムオペレーティングシステムが採用されている。

【0023】当然のこととして組み込まれる装置毎に異なる専用のオペレーティングシステムの開発費用は大きい。そのため、最近ではエンベデッド（組み込み）用のリアルタイムオペレーティングシステムとしてパーソナルコンピュータ用の汎用オペレーティングシステムを転用することが提案されており、マイクロカーネルと組み合わされるサブシステムにエンベデッド用の固有のプログラムを配置することにより、組み込み用のリアルタイムオペレーティングシステムを得ることが行われている。

【0024】オペレーティングシステムの大きな機能としてスケジューリングや割り込み処理等のタスク管理がある。タスク管理に関して、オペレーティングシステムには大きく分けて同時に 1 つのタスク処理しか行わないシングルタスク方式と、同時に複数のタスク処理を行うマルチタスク方式があり、マルチタスク方式はさらにタスクの切り替えが処理されるタスクに依存するマルチタスク方式と、処理されるタスクに依存しないマルチタスク方式に区分される。

【0025】これらの中、シングルタスク方式は MPU に 1 つのプロセスを割り当てそのプロセスが終了するまで MPU を解放しないものであり、ノンプリエンプティブマルチタスク方式は MPU を時分割して複数のプロセスに割り当てることができるが、実行中のプロセスがオペレーティングシステムに制御を戻さない限り他のプロセスは実行されないものであり、プリエンプティブマルチタスク方式はある時間間隔で実行中のプロセスに割り込みを行い、他のプロセスに強制的に制御を移すものである。したがって、リアルタイムのマルチタスクはプリエンプティブ方式の場合にのみ可能である。

【0026】コンピュータにおけるタスク管理はメモリやファイルなどのシステム資源を持つ単位であるプロセスに基づいて行われ、プロセスの管理はプロセスを細分化した CPU 時間を割り当てる単位であるスレッドに基づいて行われる。なお、この場合システム資源は同一プロセス内の全てのスレッドで共有され、したがって一つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

【0027】マルチタスク方式で処理される各タスクには優先順位（Priority Spectrum）があり、一般的には 3 2 の段階に分けられる。この場合、割り込みを行わない通常のタスクは 0 - 1 5 段階に分けられるダイナミッククラス（Dynamic Classes）に区分され、割り込みを行うタスクは 1 6 - 3 1 段階に分けられるリアルタイムクラス（Real-Time Classes）に区分される。割り込み処理はタイムスライスと呼ばれる割り込み可能時間（通常 1 0 ms）を単位として行われ通常の割り込みは 1 0 ms のタイ

ムスライスで行われている。このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が  $100\mu\text{s}$  であるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の  $10\text{ms}$  の割り込みよりも優先して割り込みが可能である。

【0028】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス 683 号, p. 99~124 に「電子透かし」がマルチメディア時代を守る」(1997/2/24, 日経BP社刊)に全般的に紹介されており、また同号, p. 149~162, ウォルター・ベンダー他「電子透かしを支えるデータ・ハイディング技術(上)」及び684号, p. 155~168, 「電子透かしを支えるデータ・ハイディング技術(下)」(IBM System Journal, vol.35, nos.3 & 4(International Business Machines Corporation)から転載)にも紹介されている。この電子透かし技術については、EP 649074にも述べられている。

#### 【0029】

【発明の概要】本件出願においては、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提案する。

【0030】本出願で提案するデジタルコンテンツ管理システムでは、ネットワークあるいはデータ放送を利用して著作権主張がされたデジタルコンテンツの不正利用を監視する。デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、著作権主張がされたデジタルコンテンツの利用はこのデジタルコンテンツ管理プログラムによって管理される。

【0031】ユーザ装置は、利用監視プログラムとリンクするデジタルコンテンツ管理プログラムの管理下に置かれ、利用監視プログラムはデジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして動作する。この利用監視プログラムは著作権主張がされたデジタルコンテンツの不正利用を監視し、不正利用が行われている場合には、利用の停止、警告あるいはデジタルコンテンツへの可視電子透かしの埋め込みを行う。また、正規利用の場合にも利用状況の追跡を行うために可視電子透かしに代えて不可視電子透かしを埋め込むことができる。

【0032】さらに、本出願では公開鍵をネットワークあるいは放送により配布するシステムを提案する。公開鍵は公開鍵配布画面に記入されて配布されるが、公開鍵

配布画面には公開鍵所有者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されている。利用者が公開鍵配布画面を公開鍵管理センタに提示すると公開鍵管理センタが不可視電子透かしにより公開鍵所有者の正当性を確認する。

【0033】公開鍵をネットワークにより配布する場合には、公開鍵所有者の情報あるいは公開鍵を請求したユーザの情報を不可視電子透かしとして埋め込み、埋め込まれた不可視電子透かしを確認することにより、公開鍵の正当性あるいはユーザの正当性を確認することができる。その場合、ユーザの情報としてユーザの公開鍵の電子指紋を利用すれば、確認が容易になる。

#### 【0034】

【実施例】図面を用いて本願発明の実施例を説明する。デジタルコンテンツの著作権保護においてはユーザ側装置での不正利用を如何に防止するかが最大の課題であり、特開平 7-271865 号の「データベース著作権管理方法」ではこれを目的としてデジタルコンテンツ管理プログラムにより復号/再暗号及び利用制限が行われる。しかしながら、著作権保護の対象であるデジタルコンテンツはユーザ側装置によって復号/再暗号が行われるため、復号/再暗号の処理及びそのために使用される暗号鍵の管理が万全であることは期しがたく、デジタルコンテンツ管理プログラムを無効化することによりデジタルコンテンツが不正に保存・複写・転送・加工される可能性がある。

【0035】このような不正利用を制限するためには、デジタルコンテンツの復号/再暗号処理及び暗号鍵の管理を行うデジタルコンテンツ管理プログラムがユーザによって改変されないようにする必要があり、そのためにはデジタルコンテンツ管理プログラムのハードウェア(ファームウェア)化が最も確実な方法である。例えば、現在アナログテレビジョン放送においてスクランブルされた放送番組のデスクランブルに使用されている専用のスクランブルデコーダのような専用のデジタルコンテンツ管理装置を使用することによってのみデジタルコンテンツの復号/再暗号処理及び暗号鍵の管理が可能にする構成がある。

【0036】このような構成は確実ではあるがシステム構成が柔軟性に欠けており、ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合に、ユーザがこれらの変更に対応することは大変である。

【0037】ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合であっても、柔軟に対処するためにはデジタルコンテンツ管理プログラムがソフトウェアであることが望ましいが、デジタルコンテンツ管理プログラムがアプリケーションプログラムである場合には改変が行われる可能性がある。したがって、デジタルコンテンツ管理プログラムがソフト

ウェアであるためには、ユーザが改変を行うことができないオペレーティングシステム（OS）の固定領域であるカーネルにデジタルコンテンツ管理プログラムを組み込む必要がある。

【0038】しかし、カーネルという固定領域にデジタルコンテンツ管理プログラムを組み込んだ場合には、データベースによってデジタルコンテンツ管理システム及び暗号システムが異なっているような場合に現実的ではない。

【0039】前に述べたように、リアルタイムオペレーティングシステムにはカーネル領域も含む他のオペレーティングシステム内のシステムのタイムスライス時間よりも1～2桁早いリアルタイムスライス時間で割り込み動作可能なものがあり、この技術を利用することにより、全体の動作に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視し、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。次にリアルタイムオペレーティングシステムを利用してデジタルコンテンツ管理プログラムを補強する方法を説明する。

【0040】デジタルコンテンツの不正利用は復号されたデジタルコンテンツの無許可加工、無許可保存、無許可複製あるいは無許可転送することによって行われるから、不正利用の有無は復号化デジタルコンテンツの加工、保存、複製あるいは転送の有無によって検出することができる。そのために、不正利用を監視するプロセスは、ある時間間隔でデジタルコンテンツ管理プログラムが実行中のプロセスに割り込みを行い、強制的に監視を行うプリエンティブ方式のマルチタスクにより割り込みを行う。

【0041】通常使用されるマルチタスクタイムスライスは10msであり、復号／再暗号プロセスもこの時間単位で行われる。一方、最速のリアルタイムスライスは1/100の100μsである。したがって、復号されたデジタルコンテンツが加工、保存、複製あるいはアップロードされているかを割り込み優先順位の高い監視タスクにより監視することにより、ユーザが行っている正当な利用に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視することができ、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。

【0042】このような監視機能を有するデジタルコンテンツ管理プログラムはオペレーティングシステムのカーネル部分ではなくユーザモードで動作するサブシステム領域に組み込み、監視プロセスは優先順位の高いプロセスとする。

【0043】この構成により、復号／再暗号によるデジタルコンテンツの利用と許可外の不正利用の有無の監視を同時に、かつ円滑に実行することができる。

【0044】図1に、デジタルコンテンツ管理プログラ

ムが組み込まれたオペレーティングシステムの構成を示す。このオペレーティングシステムはユーザが操作することができないカーネルモードで動作する管理部(Executive)と、ユーザが操作することができるユーザモードで動作するサブシステムからなり、管理部とサブシステムとはシステムサービスAPI(Application Programming Interface)によってインターフェースされており、ハードウェアとカーネル部の間にはHAL(Hardware abstraction Layer)が介在している。

【0045】サブシステムは、他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステム及びセキュリティサブシステム等の中枢サブシステムとアプリケーションプログラムから構成されている。

【0046】管理部には、マイクロカーネル(micro kernel)である仮想記憶管理機能(virtual memory manager)、オブジェクトマネージャ、LPC(Local Procedure Call)機能、プロセスマネージャ、セキュリティ参照モニタと、最も基本的な要素であるカーネルとディスク及びネットワークとの間の入出力を管理するI/O管理機能(I/O manager)に、さらに著作権主張がされたデジタルコンテンツの管理を行うデジタルコンテンツ管理プログラム、すなわちデジタルコンテンツ管理機能(digital content manager)が組み込まれており、デジタルコンテンツの管理における重要な部分である保存、複製あるいは転送の管理はデジタルコンテンツ管理機能がI/O管理機能を管理することによって行われる。

【0047】図2に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの実施例である。このデジタルコンテンツ管理システムにおいて、ユーザによるデジタルコンテンツ利用状況の監視はネットワークを介して行われる。この図において、1はデータベース、2はデジタルコンテンツ管理センタ、4はユーザであり、ユーザ4とデータベース1及びデジタルコンテンツ管理センタ2は公衆通信回線あるいは双方向性CATV回線であるネットワーク3で接続されている。

【0048】データベース1にはデジタルコンテンツが蓄積されており、破線で示された経路5を経由して暗号化デジタルコンテンツがユーザ4に転送される。データベース1は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を経路6によりデジタルコンテンツ管理センタ2に転送し、デジタルコンテンツ管理センタ2は転送された復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線7で示された経路を経由してユーザ4に配送する。また、デジタルコンテンツ管理センタ2は監視プログラムを実線で示された経路8でユーザ4に送信する。

【0049】利用許可内容はユーザ4が使用する装置に組み込まれているデジタルコンテンツ管理プログラムによって管理されているが、悪意のあるユーザによってデ



デジタルコンテンツ管理プログラムが管理している範囲外の利用が行われる可能性を完全には否定することができない。デジタルコンテンツ管理プログラムはユーザ4の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理されており、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。しかし、悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【0050】監視プログラムはユーザ4が使用する装置に組み込まれているデジタルコンテンツ管理プログラムとリンクしてデジタルコンテンツ管理プログラムの処理に割り込むことにより監視動作を行い、ユーザが利用許可内容を越えた利用を行なっているかどうかを監視し、このような不正利用である保存・複写・転送が行われていることを検知した監視プログラムは特開平7-271865号に示された警告の表示に代えて、復号処理の停止、ユーザが関知しない暗号鍵による強制再暗号化あるいは図3(a)に示された原デジタルコンテンツへの図3(b)に示された可視電子透かしの埋め込み、あるいは図4(b)に示された不可視電子透かしのデジタルコンテンツへの埋め込みを行う。

【0051】ここで利用許可内容というのは、デジタルコンテンツの、単純利用、内蔵記憶装置への保存、外部媒体への複写、ネットワークを経由しての他の利用者への転送を指す。なお、可視電子透かしとして埋め込まれるのはユーザの名前等識別容易なものが適切である。

【0052】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視プログラムが協働している。言い換えれば、監視プログラムと協働していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、ネットワークを経由して監視プログラムが起動していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテンツ管理プログラムを起動させると自動的にネットワークを経由して監視プログラムが起動されるようにされている。ユーザがネットワーク経由でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視プログラムも転送される。

【0053】なお、監視プログラムをデジタルコンテンツ管理プログラムに一体化し、デジタルコンテンツ管理プログラムに監視動作を行わせる監視コマンドを送信してデジタルコンテンツ管理プログラムに監視動作を行わせるようにすることもできる。

【0054】ネットワークを介して行うデジタルコンテンツ管理システムにおいて、画像データ等情報量の多い

デジタルコンテンツを扱う場合には、通信回線としてISDN(Integrated System for Digital Network)回線を使用することが多い。このISDN回線として一般的に使用されているものは、Bチャンネルと呼ばれるデータ伝送速度が64Kbpsであるデータチャンネルが2チャンネル、Dチャンネルと呼ばれるデータ伝送速度が16Kbpsである制御チャンネルが1チャンネルあり、当然のこととしてデジタルコンテンツは1~2チャンネルのデータチャンネルで伝送されるが、Dチャンネルは使用されていないことが多い。そこで、監視プログラムによる割り込み監視をこのDチャンネルで行うことによれば、デジタルコンテンツの使用に全く影響与えることなく、利用状況の遠隔監視を行うことが可能になる。

【0055】また、公衆通信回線を使用する場合にはダウンロード用に最大56Kbpsのデータ伝送速度を実現することができるADSL(asymmetric digital subscriber line)技術を利用することにより、監視プログラムによる割り込み監視を効率的に行うことができる。

【0056】図4に示すのは、利用許可内容に含まれている正規の保存・複写・転送の場合であっても電子透かしを埋め込む例である。この場合の電子透かしは、電子透かし検出手段によって(b)のように検出される不可視電子透かしであって、電子透かし検出手段によらない場合は(a)に示されたように原デジタルコンテンツと一見代わりはない。なお、可視電子透かしの場合と同様に埋め込まれるのはユーザの名前等識別容易なものが適切である。

【0057】このようにすることにより、初めは正規利用であっても後で不正利用が行われた場合に保存・複写・転送の経路を確認することができる。また、正規のものであっても保存・複写・転送が繰り返されることにより、(c)に示されたように不可視電子透かしが増え、その結果デジタルコンテンツの品質が低下する。このようなことによって無限に保存・複写・転送が繰り返されることがなくなり、デジタルコンテンツの管理が容易になる。

【0058】デジタルコンテンツ管理のために重要な要素である「再暗号化」はユーザの装置にとってかなり負担の重いプロセスである。そのため、簡易型として電子透かしを埋め込むだけでもデジタルコンテンツの不正利用を防止するには有効である。

【0059】デジタルコンテンツの利用が有料で行われる場合に、特開平7-271865号に示されているようにユーザが予め利用許可鍵を入手するようにすれば、課金は容易に行われるが、デジタルコンテンツ管理センタが利用実績であるメータリングデータを後でポーリングによって回収して課金を行う場合には、ポーリングが行われるまでメータリングデータはユーザの管理下におかれる。そのため、悪意あるユーザによってメータリングデータの改竄が行われ、正常な課金が妨げられること

が考えられる。

【0060】この実施例のデジタルコンテンツ管理システムにおいてはユーザがデジタルコンテンツを利用してゐる時にはユーザ装置は常に管理センタに接続され、監視プログラムによる利用状況の監視が行われている。したがって、この監視動作の中でメタリングデータをデジタルコンテンツ管理センタに保管することにより、ポーリングの必要がなくなり、ユーザによるメタリングデータの改竄を防止することができる。また、デジタルコンテンツの利用が無料で行われる場合であっても、ユーザによる利用状況を容易に把握することができる。

【0061】図5に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの他の実施例の構成図である。このデジタルコンテンツ管理システムにおいて、デジタルコンテンツ利用状況の監視は放送によって行われる。この図において、11はデータベース、12はデジタルコンテンツ管理センタ、14はユーザであり、ユーザ14とデータベース1及びデジタルコンテンツ管理センタ12は公衆通信回線あるいは双方向性CATV回線であるネットワーク13で接続されている。

【0062】データベース11にはデジタルコンテンツが蓄積されており、破線で示された経路15を経由して暗号化デジタルコンテンツがユーザ14に転送される。デジタルコンテンツ管理センタ12は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線17で示された経路を経由してユーザ14に配送する。また、デジタルコンテンツ管理センタ12は監視コマンドを放送局19に転送し、放送局19は転送された監視コマンドを実線で示された経路18でユーザ14に送信する。

【0063】この経路18は放送電波が最も一般的であるが、有線放送であるCATVケーブルも利用可能であり、さらにインターネット放送が行われている場合にはネットワークを利用することも可能である。

【0064】この監視コマンドはユーザ14が使用する装置に組み込まれているデジタルコンテンツ管理プログラムが行っている動作に割り込み、ユーザが利用許可内容を越えた利用を行なっているかどうかをデジタルコンテンツ管理プログラムに監視させ、保存・複写・転送が行われるときには復号処理を停止させ、あるいは図3に示された可視電子透かし又は図4に示された不可視電子透かしをデジタルコンテンツに埋め込む。

【0065】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視コマンドが割り込み動作を行っている。言い換えれば、監視コマンドが放送されている放送波を受信していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、放送波を経由して監視コマンドを受信していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテ

ツ管理プログラムを起動させると自動的に放送波を経由する監視コマンドを受信する。ユーザがデータ放送等でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視コマンドも転送される。

【0066】デジタルコンテンツ管理プログラムはユーザ14の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理され、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【0067】このような不正規の利用が行われていることを検知した監視プログラムは特開平7-271865号に示された警告の表示に代えて、図3(b)に示されたような可視電子透かしの埋め込みを行う。また、利用許可内容に含まれている正規の保存・複写・転送の場合であっても図4(b)及び(c)に示されたような、電子透かし検出手段によってはじめて検出される不可視電子透かしを埋め込むことも可能である。

【0068】これらの放送あるいはネットワークを介しての監視動作は、ユーザがユーザの意志で行うのではなく、著作権主張がされたデジタルコンテンツを利用する場合にはデジタルコンテンツ管理プログラムにより自動的に行われる。さらにこの動作を確実にするには、放送あるいはネットワークを介しての監視動作が行われていない場合にはデジタルコンテンツ管理プログラムによる復号／暗号化等の動作が行われないようにされる。また、著作権主張がされたデジタルコンテンツを利用する場合には監視プログラムを放送する電波の受信あるいは監視プログラムを送信する管理センタに自動的に接続される。

【0069】次に、公開鍵の配布を行う実施例を説明する。共通鍵(common key)システムとも呼ばれる秘密鍵(secret key)システムで使用される暗号鍵の大きさは大きいものでも100ビット程度であるのに対して、公開鍵(public key)システムで使用される暗号鍵は大きいものは1000ビットを越す。公開鍵システムは安全性が高い反面暗号化／復号化に手間がかかるため、秘密鍵の送付、デジタル署名、認証等容量の小さいデータの暗号化に用いられ、デジタルコンテンツの暗号化は秘密鍵を用いて行われる。公開鍵システムでは公開鍵と専用鍵(private key)が組み合わされて使用され、専用鍵は所有者の管理下におかれ、他人が知ることはできないが、公開鍵はその使用目的上、他人に知らされている必要がある。

【0070】そのために、公開鍵は種々の手段で公衆に



配布されるが、その際に所有者から直接に公開鍵を受領することができれば偽の公開鍵を配布される恐れは少ないが、そうでない場合には偽の公開鍵を受領してしまうことがある。この実施例では公開鍵を放送あるいはネットワークを経由するという間接的な配布方法においても配布された公開鍵の真偽を用いて確認することができるデジタルコンテンツ管理システム、いわば鍵配信ネットワークを提案する。

【0071】図6に、放送により公開鍵の配布を行うデジタルコンテンツ管理システムの本発明の実施例を示す。このデジタルコンテンツ管理システムでは、公開鍵は広く一般に配送されるため、電子商取引等における公開鍵認証方式で採用されるPEM(Privacy Enhanced Mail)方式に代わる簡易認証方式として用いることができる。

【0072】この図において、21は公開鍵所有者、22は公開鍵管理センタ、23は放送局、24はネットワーク、25はユーザである。放送局23は地上波アナログ、衛星アナログ、CATVアナログ、地上波デジタル、衛星デジタル、CATVデジタル等のテレビジョンあるいは音声放送局であり、走査線多重(Vertical Blank Interval:VBI)、音声多重、データ混入等適宜の手段によりデータ放送が行われる。なお、この放送局としてインターネット放送局も利用可能である。ネットワーク24は公衆通信回線あるいは双方向性CATV回線であり、公開鍵管理センタ22とユーザ25との間はネットワーク24で接続されており、放送局23とユーザ25との間は適宜な情報伝達媒体により接続される。

【0073】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者21は所有する公開鍵と公開鍵所有者本人であることを証明する何らかのデータを公開鍵所有者識別用データとして経路26により公開鍵管理センタ22に転送する。ここで使用される公開鍵所有者識別用データとして、公開鍵所有者名等の情報を直接に利用されるが、その情報をMD5ハッシュアルゴリズムによって16バイトのデータに縮小した電子指紋を利用することもできる。

【0074】公開鍵管理センタは図7(a)に示されたような公開鍵配布画面を用意しておき、所定の位置に公開鍵を挿入する。この画面は挿入された公開鍵を容易に分離して使用することができるようにHTML(Hyper Text Markup Language)形式あるいはXML(eXtensible Markup Language)形式を使用して作成されており、その一部にはイメージデータが挿入されている。

【0075】このイメージデータには、公開鍵所有者21の識別用データ(OWNER'S ID)が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタは図7(b)に示されたように電子透かしの内容を知ることができるが、その他

の者が見た場合には図7(a)のような通常の画面であり、電子透かしの内容を知ることにはできない。

【0076】このイメージ画面として広告を掲載しておけば公開鍵配布に要する経費を広告掲載料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータとしては写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしの埋め込むことも可能である。

【0077】放送局23は、このようにして作成された公開鍵配布画面を放送経路28により放送する。

【0078】放送された公開鍵配布画面をユーザ25が受信するが、ユーザ25が受信した公開鍵配布画面のイメージ画面に埋め込まれた電子透かしは不可視のものであるから、ユーザ25は電子透かしの内容を知ることにはできない。

【0079】ユーザ25は、放送された公開鍵配布画面から公開鍵を分離して各種電子商取引に使用するが、公開鍵の真偽に疑いを持った場合にはネットワーク24による経路29により公開鍵配布画面を公開鍵管理センタ22に転送する。

【0080】公開鍵管理センタ22は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、図7(b)に示されたように検出された公開鍵所有者の識別情報についてネットワーク24による経路30によりユーザ25に通知する。

【0081】このようにすることにより、他人が成りすましていたような場合にその成りすましを検出することができる。その場合、公開鍵所有者の識別情報として電子指紋を用いた場合には検証が極めて簡易になる。

【0082】イメージ画面には、広告以外に公開鍵所有者の意向により、図7(c)に示したような好みの画面、あるいは図7(d)に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

【0083】なお、この実施例で埋め込まれる不可視の電子透かしは公開鍵管理センタのみが確認することができるようにされているが、確認だけはユーザができるようにすることもできる。その場合、公開鍵所有者識別情報として電子指紋を用い、ユーザが公開鍵所有者に電子指紋を確認するようにすることもできる。

【0084】図8により、公開鍵がユーザの要求に応じて配布される本発明の他の実施例を説明する。図6に関して説明した放送により公開鍵を配布するデジタルコンテンツ管理システムは、主として電子商取引等不特定多数のユーザに公開鍵を配布する場合に有効なシステムである。これに対して、個人的なメールを送付する場合には公開鍵を配布する相手は特定少数であることが多く、

放送によって配布する必要はない。図 8 に示されたデジタルコンテンツ管理システムでは、公開鍵はネットワークを経由して個別に配送されるため、電子メール等における公開鍵認証方式で採用される PGP (Pretty Good Privacy) 方式に代わる簡易認証方式として用いることができる。

【0085】この図において、31 は公開鍵所有者、32 は公開鍵管理センタ、33 はネットワーク、34 はユーザである。ネットワーク 33 は公衆通信回線あるいは双方向性 CATV 回線であり、公開鍵所有者 31 とユーザ 34 との間及び公開鍵管理センタ 32 とユーザ 34 との間はネットワーク 33 で接続されており、公開鍵所有者 31 と公開鍵管理センタ 32 との間は適宜な情報伝達手段により接続される。

【0086】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者 31 は所有する公開鍵と公開鍵所有者識別用データとして公開鍵所有者本人であることを証明する何らかのデータをネットワーク 33 を経由する経路 35 により公開鍵管理センタ 32 に転送する。

【0087】公開鍵管理センタ 32 は図 7 (a) に示された公開鍵配布画面の所定の位置に公開鍵を挿入するとともに公開鍵配布画面のイメージ画面に公開鍵所有者識別データを不可視電子透かしとして埋め込んで、経路 36 により公開鍵所有者 31 に返送する。なお、このデジタルコンテンツ管理システムにおいても使用される公開鍵所有者識別用データ及び公開鍵配布画面は、図 6 に示されたデジタルコンテンツ管理システムの場合と同一であるため、ここでの再度の説明は省略する。

【0088】公開鍵所有者 31 の公開鍵を入手しようとするユーザ 34 はネットワーク 33 を経由して経路 37 により公開鍵所有者 31 に公開鍵の配布を依頼し、この依頼に応じて公開鍵所有者 31 はネットワーク 33 を経由する経路 38 により公開鍵配布画面をユーザ 34 に転送する。

【0089】ユーザ 34 は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて電子メールを暗号化し、公開鍵所有者 31 に送信する。公開鍵所有者 31 は、暗号化メールを所有する専用鍵を用いて復号する。

【0090】ユーザ 34 が、転送された公開鍵の真偽に疑いを持った場合には経路 39 により転送された公開鍵配布画面を公開鍵管理センタ 32 に転送する。公開鍵管理センタ 32 は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路 40 によりユーザ 34 に通知する。このようにすることにより、他人が公開鍵所有者 31 に成りすましていたような場合にその成りすましを検出することができる。

【0091】この実施例では、公開鍵配布画面を公開鍵

所有者 31 がユーザ 34 に直接に配布しているが、この他に公開鍵配布画面を公開鍵管理センタ 32 が管理し、配布するように構成することもできる。

【0092】図 9 及び図 10 により、公開鍵がユーザの要求に応じて配布される本発明のさらに他の実施例を説明する。この実施例では、電子商取引用の公開鍵を取り扱う。図 6 に示された実施例及び図 8 に示された実施例では、電子透かしを用いて公開鍵所有者の検証を行っているが、図 9 及び図 10 に示された実施例では、公開鍵使用者の検証を行う。

【0093】図 9 に示されたデジタルコンテンツ管理システムにおいて、41 は公開鍵所有者、42 は公開鍵管理センタ、43 はネットワーク、44 はユーザである。ネットワーク 43 は公衆通信回線あるいは双方向性 CATV 回線であり、公開鍵所有者 41 とユーザ 44 との間、公開鍵所有者 41 と公開鍵管理センタ 42 との間、ユーザ 44 と公開鍵管理センタ 42 との間はネットワーク 43 により各々接続される。

【0094】このように構成されたデジタルコンテンツ管理システムにおいて、初めに公開鍵所有者 41 は所有する公開鍵を経路 45 により公開鍵管理センタ 42 に転送し、公開鍵管理センタ 42 は転送された公開鍵を保管している。公開鍵所有者 41 に対して電子商取引で発注等の行為を行おうとするユーザ 44 は、ユーザ 44 の身元を証明する何らかのユーザ識別データをネットワーク 43 を経由する経路 46 により公開鍵管理センタ 42 に転送する。

【0095】公開鍵管理センタ 42 は図 10 (a) に示された公開鍵配布画面の所定の公開鍵挿入位置に公開鍵を挿入するとともに図 10 (b) に示されたように公開鍵配布画面のイメージ画面にユーザ 44 の識別データを不可視の電子透かしとして埋め込んで、ネットワーク 43 を経由する経路 47 によりユーザ 44 に転送する。

【0096】ここで使用するユーザ識別用データとして、ユーザ名等の情報を直接に利用することも可能であるが、その情報を MD5 ハッシュアルゴリズムによって 16 バイトのデータに縮小した電子指紋を利用することができる。

【0097】公開鍵配布画面は挿入された公開鍵を容易に分離することができるように HTML 形式あるいは XML 形式を使用して作成されており、その一部にはイメージデータが挿入されている。このイメージデータには、ユーザ 44 の識別データ (USER'S ID) が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタが確認する場合には図 10 (b) のように内容を知ることができるが、その他の者が見た場合には図 10 (a) のような通常の画面であり、電子透かしの内容を知ることとはできない。

【0098】このイメージ画面は広告にしておけば公開

鍵配布に要する経費を広告料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータは写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしを埋め込むことも可能である。

【0099】ユーザ44は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて発注書を暗号化し、転送された公開鍵配布画面とともに公開鍵所有者41に送信する。公開鍵所有者41は、暗号化発注書を所有する専用鍵を用いて復号し、受注業務を行う。

【0100】公開鍵所有者41が発注者の真偽に疑いを持った場合には、ネットワーク43を経由する経路48により送信された公開鍵配布画面を公開鍵管理センタ42に転送する。公開鍵管理センタ42は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路49により公開鍵所有者41に通知する。このようにすることにより、ユーザ44に他人が成りすましていたような場合に、その成りすましを検出することができる。

【0101】イメージ画面には、広告以外に公開鍵所有者の意向により、図10(c)に示したような好みの画面、あるいは図10(d)に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

#### 【図面の簡単な説明】

【図1】本発明で使用されるデジタルコンテンツ管理機能付きオペレーティングシステムの構成概念図。

【図2】デジタルコンテンツの不正利用監視を行う本発

明のデジタルデータ管理システムの構成図。

【図3】本発明のデジタルデータ管理システムによる管理状態の説明図。

【図4】本発明のデジタルデータ管理システムによる他の管理状態の説明図。

【図5】デジタルコンテンツの不正利用監視を行う本発明の他のデジタルデータ管理システムの構成図。

【図6】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のデジタルデータ管理システムの構成図。

【図7】図6のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

【図8】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明の他のデジタルデータ管理システムの構成図。

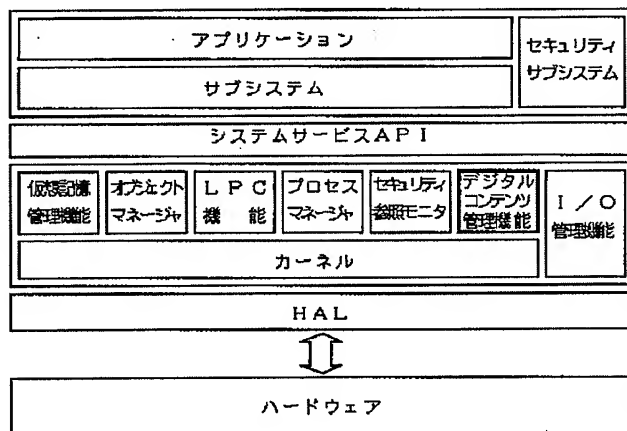
【図9】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のさらに他のデジタルデータ管理システムの構成図。

【図10】図9のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

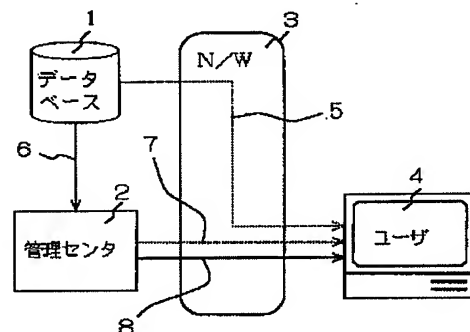
#### 【符号の説明】

- 1 データベース
- 2 デジタルコンテンツ管理センタ
- 3, 13, 24, 33, 43 ネットワーク
- 4, 14, 25, 34, 44 ユーザ
- 11 データベース
- 12 デジタルコンテンツ管理センタ
- 19, 23 放送局
- 21, 31, 41 公開鍵所有者
- 22, 32, 42 公開鍵管理センタ

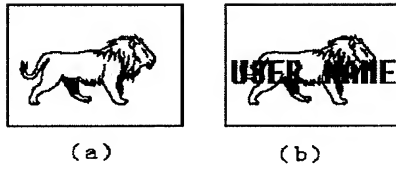
【図1】



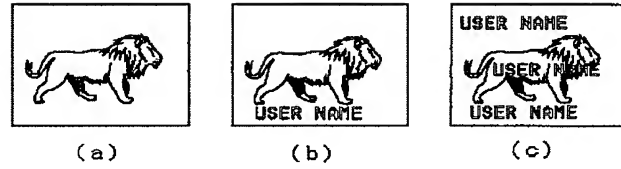
【図2】



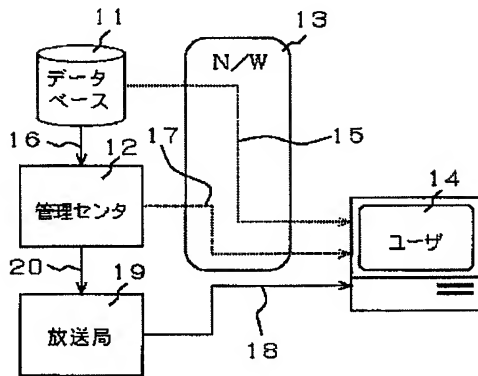
【図3】



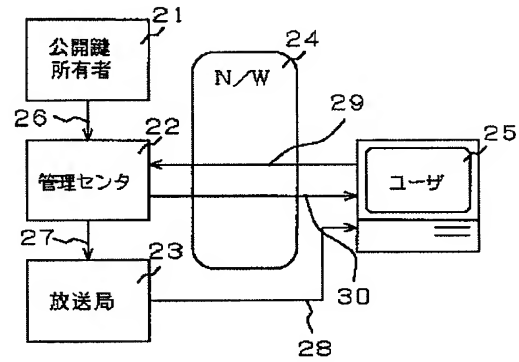
【図4】



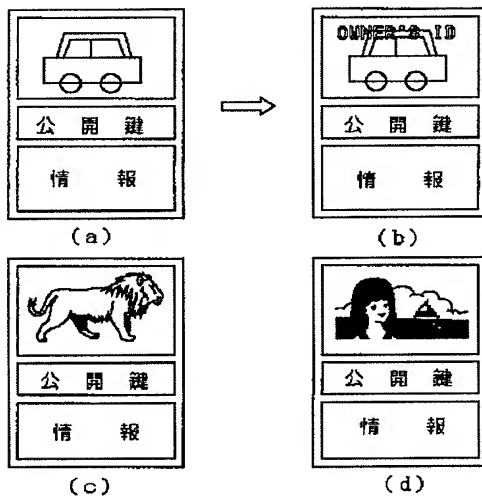
【図5】



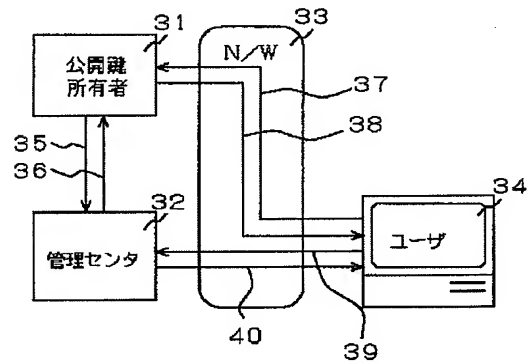
【図6】



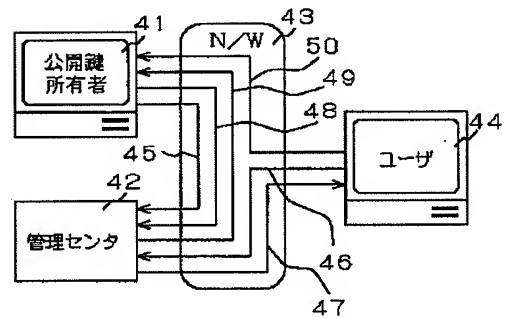
【図7】



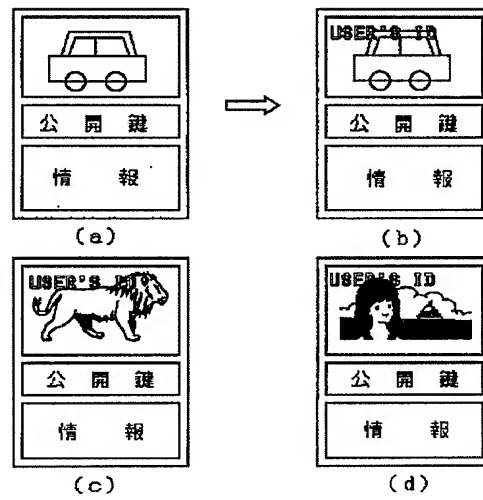
【図8】



【図9】



【図 10】



# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-007241

(43)Date of publication of application : 12.01.1999

---

(51)Int.Cl. G09C 5/00  
G06F 12/14  
G09C 1/00  
H04N 7/08  
H04N 7/081

---

(21)Application number : 09-173168 (71)Applicant : MITSUBISHI CORP

(22)Date of filing : 13.06.1997 (72)Inventor : SAITO MAKOTO

---

## (54) DIGITAL CONTENTS CONTROL SYSTEM USING ELECTRONIC WATERMARK

### (57)Abstract:

PROBLEM TO BE SOLVED: To prevent an unjust use on a user side device in the protection of the copy-right of digital contents by operating a use monitoring program as a process with priority higher than a digital contents control program. SOLUTION: A data base 1 transfers ciphered digital contents to a user 4 through a network 3. Furtherit transfers a cipher key for deciphering/ deciphering the ciphered digital contents to a digital contents control center 2. The control center 2 ciphers the cipher key to transmit it to the user 4. Furtherthe control center 2 transmits a monitoring program to the user 4. The digital contents control program incorporated in a device used by the user 4 controls the preservation/copy/transfer of the digital contents. The monitoring program interrupting into the control program detects that the preservation/copy/transfer being an irregular use are performed and embeds a visible electronic watermark in the original digital contents.

---

## CLAIMS

---

### [Claim(s)]

[Claim 1]A copyright opinion is a digital-contents managerial system which manages made digital contentsand the :aforementioned digital-contents managerial systemA digital contents control program is incorporated as a microkernel into an operating system of a user's deviceand the; aforementioned digital contents control program and a use monitoring program to link by broadcast. It is transmitted to said user's unit and said use monitoring program supervises



Assessment on Search Report by Designated Searching Authority of said digital contents as a process that interrupt priority is higher than the; aforementioned digital contents control program.

[Claim 2]The digital-contents managerial system according to claim 1 which embeds said user's information as a visible watermark at said digital contents when an illegal use is detected as said Assessment on Search Report by Designated Searching Authority.

[Claim 3]The digital-contents managerial system according to claim 1 which embeds said user's information as an invisible watermark at said digital contents when an illegal use is detected as said Assessment on Search Report by Designated Searching Authority.

[Claim 4]The digital-contents managerial system according to claim 1 which embeds said user's information as an invisible watermark at said digital contents when preservation and a copyand/or \*\*\*\*\* are detected as said Assessment on Search Report by Designated Searching Authority.

[Claim 5]To a user a public key control center is a digital-contents managerial system which delivers a public key and the ;aforementioned digital-contents managerial systemSaid public key is entered in a public key distribution screen and is distributed by broadcast image information is attached to the; aforementioned public key distribution screen and information of an owner of said public key to the; aforementioned image information as invisible digital watermarking. If it is embedded the; aforementioned user separates and uses said public key from said public key distribution screen and the; aforementioned user shows said public key control center said public key distribution screen said public key control center will check a public key owner by said invisible digital watermarking.

[Claim 6]The digital-contents managerial system according to claim 5 with which electronic fingerprints of information of an owner of said public key are used as information of an owner of said public key.

[Claim 7]To a user a public key control center is a digital-contents managerial system which delivers a public key and the ;aforementioned digital-contents managerial systemSaid user demands distribution of said public key of said public key control center and the; aforementioned public key control center enters said public key in a public key distribution screen. Supply said user widely image information is attached to the; aforementioned public key distribution screen and information of an owner of said public key to the; aforementioned image information as invisible digital watermarking. If it is embedded the; aforementioned user separates and uses said public key from said public key distribution screen and the; aforementioned user shows said public key control center said public key distribution screen said public key control center will check an owner of said public key by said invisible digital watermarking.

[Claim 8]The digital-contents managerial system according to claim 7 with which it replaces with information of an owner of said public key and electronic fingerprints of information of an owner of said public key are used.

[Claim 9]To a user a public key control center is a digital-contents managerial

system which delivers a public key and the aforementioned digital-contents managerial system. Said user shows said public key control center said user's information. Require distribution of said public key and the; aforementioned public key control center enters said public key in a public key distribution screen. Supply said user widely image information is attached to the; aforementioned public key distribution screen said user's information is embedded as invisible digital watermarking at the; aforementioned image information and the; aforementioned user separates said public key from said public key distribution screen. If said public key distribution screen is transmitted to an owner of said public key and an owner of the; aforementioned public key shows said public key distribution screen to said public key control center with digital contents enciphered using said public key said public key control center will check said user by said invisible digital watermarking. [Claim 10] The digital-contents managerial system according to claim 9 with which it replaces with said user and electronic fingerprints of said user's information are used.

---

## DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Application of the Invention] This invention relates to the system which performs management of digital contents especially copyright management of the digital contents which the copyright opinion was made and security of digital contents.

[0002]

[Description of the Prior Art] The database system which uses mutually various kinds of data which each computer saved independently by connecting each computer by a communication line until now today when it is called the information age is spreading. encoded information with little amount of information to the information which set to this database system and has been treated by until which can be processed by classic computer — and it being monochrome binary data like facsimile information and in \*\* and time at most the amount of information like natural drawing and an animation could not be markedly alike and many data was not able to be dealt with.

[0003] By the way while the digital processing art of various electrical signals develops development of digital processing art is conventionally furthered also for picture signals other than the binary data currently treated only as an analog signal. Since it becomes possible to treat a picture signal like a television signal by computer by digitization of this picture signal the "multi-media system" which deals with simultaneously the data of the various kinds which a computer treats and the image data which digitized the picture signal attracts attention as future art.

[0004] Since quality deteriorated whenever the analog content which has spread widely conventionally carries out preservation copy processing and

transmissionprocessing of the copyright produced according to these work did not become a big problem. Howeversince quality degradation does not produce digital contents even if they repeat preservationa copyprocessingand transmission and perform themprocessing of the copyright produced according to these work is a big problem. Until nowthere is no exact method in the copyright processing of digital contentsand it is the Copyright Actor is processed by the contractand the compensation to the sound recording and picture recording apparatus of a digital system is only institutionalized also in the Copyright Act.

[0005]The directions of a database are used effectively by it not only referring to the contentsbut savingcopying and processing the usually obtained digital contentsIt is even possible to be on-lineor to transmit to othersor to transmit the processed digital contents to a database using a suitable storagevia a communication linefurther off-lineand to register as new data. Although only alphabetic data had been applicable in the conventional database systemIn a multi-media systemin addition to Hitoshi Monju's data put in a database until nowthe voice data and the image data which are originally analog content are digital-contents-izedand let them be a database.

[0006]In such a situationalthough how the copyright of the digital contents put in a database is dealt with poses a big problema copyright management means for that and the copyright management means in particular completed about secondary use of a copyprocessingtransmissionetc. are not the place which is the former. Although the digital contents called software with an advertisement or freeware do not need a usage fee in principle in usecopyright exists and may receive the restriction on copyright depending on the method of use.

[0007]In view of such a situationit aimed this invention person at protecting the copyright of digital contents until nowand he has performed various proposals to until. This invention persons proposed the device for it for the system which performs copyright management by JPH6-132916A by a permission key coming to hand from a lock management center through a public telephone and telegraph circuit by JPH6-46419A and JPH6-141004A.

[0008]In JPH7-271865A and JPH8-185448Ait proposed about the system which manages the copyright of digital contents. In these systems and devicesthose who wish viewing and listening of the enciphered program make a viewing-and-listening application to a control center via a communication line using a communication apparatusand a control center performs accounting and collects a fee while it transmits a permission key to this viewing-and-listening application. The receiving set into which the viewing-and-listening candidate who received the permission key sent the permission key into the receiving set by on-line or an off-line meansand the permission key was sent cancels the code of the program enciphered with the permission key.

[0009]The system indicated to JPH7-271865AIn order to manage the copyright in the display (sound-ization is included) of the digital contents in database system also including the real time transmission of digital image contentspreservationa copyprocessingand transmissionThe program and copyright information for

managing copyright other than the key which permits use are used. This copyright management program manages by supervising so that use which applies or is contrary to the contents of permission may not be performed.

[0010]This JPH7-271865A is supplied from a database where digital contents are enciphered and it is decrypted by the copyright management program only at the time of a display and processing and performing preservation copy and transmission in the state where it was enciphered again is indicated. What the copyright management program itself is enciphered a copyright management program is decrypted with a permission key and the decrypted copyright management program performs decryption and encryption of copyright data for when preservation of data and use other than a display are performed adding copyright information including the information about an operator to original copyright information and saving as a history is also indicated.

[0011]Decoding / device for re-encryption and the deposition system of an encryption key which have a gestalt of the board for performing copyright management in JPH8-287014A to which this application relates a PCMCIA card or an IC card were proposed. In this application reference was made also about the Television Sub-Division meeting of the copyright management method and the application to Electronic Commerce Technology Division.

[0012]The system which performs protection of the original data copyright of processing data and processing data copyright which used two or more data in JPH8-272745A by checking the justification of an application by the digital signature to a processing program combining a secret key method and a public key system was proposed.

[0013]In JPH8-288940A various gestalten for applying a copyright management system to a database a video-on-demand (VOD) system or Electronic Commerce Technology Division were proposed.

[0014]In JPH8-329011A the system which performs copyright protection of the original data in the case of using and processing two or more data and new data using the third encryption key and copyright label was proposed.

[0015]Management of data copyright is realized by performing restriction of encryption / decryption / re-encryption and the contents of use by a copyright management program so that I may be understood from the data copyright management system and data copyright management device which this invention person who explained above has proposed. This encoding technology and use restrictions are realized by using a computer.

[0016]When exchanging confidential information via a network encryption of information is performed for the prevention from theft. Preventing the information theft at the time of transmission by encryption is stated to USP5504818 and 5515441 In that case using two or more encryption keys is stated to USP5504816 and 5353351 5475757 and 5381480 and performing re-encryption is stated to USP5479514.

[0017]In order to use a computer efficiently the operating system (OS) which generalizes operation of the whole computer is used. The conventional operating

system currently used with the personal computer etc. comprised operating system service treating kernel (Kernel) treating fundamental service called memory management task management interruption and interprocess communication and other services.

[0018] However the ability improvement of a microprocessor and the change in the situation by the side of a computer called the fall of the RAM price used as a main memory unit Also in the operating system which generalizes operation of the whole computer with improvement in the military requirement from a user to a computer the improvement in functional was required and the scale of an operating system has got fat as compared with before.

[0019] In order that such an enlarged operating system may occupy the big space of a hard disk whose operating system itself is the preservation place The situation where the space where the application program or data which a user needs is saved becomes needy and the user-friendliness of a computer worsens occurs.

[0020] The environmental subsystem with which the newest operating system performs the emulation of other operating systems and screen drawing from a kernel in order to cope with such a situation It removes as the subsystem (Sub system) which is a portion which depends on a user for central subsystems such as a security subsystem HAL which absorbs the difference of hardware (Hardware abstraction Layer) Fundamental portions such as a scheduling function an interruption function and an I/O controlling function are made into the microkernel (Micro kernel) System service API (Application Programming Interface) is made to intervene between a subsystem and a microkernel and the operating system is constituted.

[0021] While the extendibility of the operating system by the function change or addition improves by doing in this way the transplantation corresponding to a use becomes easy. It becomes easy to realize a distribution operating system by distributing to two or more computers which had the element of a microkernel connected by network.

[0022] In addition to the personal computer represented by a desktop type or the note type the computer is used for computer-related peripherals various control devices a transmitter etc. In that case it differs from the general-purpose operating system for personal computers with which man-machine interface is thought as important as a specialized operating system for one embedded (inclusion) which suits each device The real time operating system with which the earliness of execution is thought as important is adopted.

[0023] The exploitation cost of a different operating system for exclusive use for every device incorporated as a matter of course is large. Therefore diverting the general-purpose operating system for personal computers to some other purpose as a real time operating system for embedded (inclusion) one these days is proposed the subsystem combined with a microkernel -- embedded one -- by arranging the peculiar program of business obtaining the real time operating system for inclusion is performed.

[0024] Task managements such as scheduling and interruption processing occurs as a

big function of an operating system. The single task method which roughly divides into an operating system and performs only one tasking simultaneously about task management. There is multitasking which performs two or more tasking simultaneously and multitasking is classified into multitasking depending on the task by which the change of a task is processed further and multitasking independent of the task processed.

[0025] Although MPU is not released in these until a single task method assigns one process to MPU and the process is completed and the non-preemptive-multitasking method can carry out the time sharing of the MPU and can assign it to two or more processes. Unless the process under execution returns control to an operating system other processes are not performed and a preemptive multitasking method interrupts the process under execution with a certain time interval and moves control to other processes compulsorily. Therefore only in the case of a preemptive method multitasking of real time is possible.

[0026] Task management in a computer is performed based on the process which is a unit with system resources such as a memory and a file and management of a process is performed based on the thread which is a unit which assigns the CPU time which subdivided the process. A system resource will be shared in this case by all the threads within the same process therefore one or more threads which share a system resource will exist in one process.

[0027] A priority (Priority Spectrum) is among each task processed with multitasking and generally it is divided into the stage of 32. In this case the usual task which does not interrupt is classified into the dynamic class (Dynamic Classes) divided into zero to 15 steps and the task which interrupts is classified into the real-time class (Real-Time Classes) divided into 16 to 31 steps. Interruption processing is performed considering the time (usually 10 ms) which is called a time slice and which can be interrupted as a unit and the usual interruption is performed by the time slice for 10 ms. In such a situation although the time slice whose time which is called a real-time slice these days and which can be interrupted is 100 microseconds was proposed if this real-time slice is used priority can be given over the conventional interruption for 10 ms and it can interrupt.

[0028] Although encoding technology is a means for making the illegal use of data contents impossible since there is no guarantee that the operation is perfect the possibility of an illegal use cannot be denied thoroughly. On the other hand although the electronic watermark technology cannot make an illegal use impossible when an illegal use is discovered it is a means although it can become final and conclusive that it is an illegal use by verifying the contents of digital watermarking. Although there are various methods "digital-watermarking" is generally introduced to the Nikkei electronics No. 683 and p.99-124 "for multimedia age to be kept" (1997/2/24\*\*\*\*BP\*\*\*\*) No. 684 besides the item p.149-162 and the Walter vendor "data hiding art (above) supporting digital watermarking" p.155-168 data hiding art supporting digital watermarking (below) (IBM System.) It is introduced also to reproduction from Journal vol.35 and nos.3 & 4 (International Business Machines Corporation). This electronic watermark technology is stated



also to EP649074.

[0029]

[Summary of Invention]In this applicationthe system which delivers the public key used for management of the system and digital contents which manage the digital contents which management of digital contentsespecially a copyright opinion were made is proposed.

[0030]In the digital-contents managerial system proposed with this applicationthe illegal use of the digital contents which the copyright opinion was made using a network or data broadcasting is supervised. It includes in the operating system of a user's unit by making a digital contents control program into a microkerneland use of the digital contents which the copyright opinion was made is managed by this digital contents control program.

[0031]A user's unit is put under management of a use monitoring program and the digital contents control program to linkand the use monitoring program operates as a process that interrupt priority is higher than a digital contents control program. This use monitoring program performs embedding of visible digital watermarking to a stopwarningor digital contents of usewhen the illegal use of the digital contents which the copyright opinion was made is supervised and the illegal use is performed. In order to pursue Assessment on Search Report by Designated Searching Authority also in regular useit can replace with visible digital watermarking and invisible digital watermarking can be embedded.

[0032]With this applicationthe system which distributes a public key by a network or broadcast is proposed. Although a public key is entered in a public key distribution screen and distributedthe image information where the public key owner's information was embedded as invisible digital watermarking is attached to the public key distribution screen. If a user shows a public key control center a public key distribution screena public key control center will check a public key owner's justification by invisible digital watermarking.

[0033]When distributing a public key with a networkthe justification of a public key or a user's justification can be checked by embedding the information of the user who charged the public key owner's information or public key as invisible digital watermarkingand checking embedded invisible digital watermarking. In that casea check will become easy if the electronic fingerprints of a user's public key are used as a user's information.

[0034]

[Example]Working example of the invention in this application is described using Drawings. It is the biggest SUBJECT how the illegal use in user side equipment is prevented in the copyright protection of digital contentsBy the "database copyright management method" of JPH7-271865Adecoding / re-codeand use restrictions are performed by the digital contents control program for the purpose of this. Howeversince decoding / re-code is performed by user side equipment as for the digital contents which are the objects of copyright protectionprocessing of decoding / re-code -- and -- thereforeit is hard to expect that management of the encryption key used is thoroughgoingand digital contents may be unjustly

savedcopiedtransmitted and processed by cancelling a digital contents control program.

[0035]In order to restrict such an illegal use a user needs to take care not to change the digital contents control program which performs decoding / re-cipher processing of digital contents and management of an encryption key. For that purpose hardware (firmware) -ization of a digital contents control program is the most positive method. For example By using a digital -contents controlling device for exclusive use like the scramble decoder for exclusive use currently used for descrambling of the program by which scramble was carried out in the present analog television broadcasting. There is composition carried out as [ be / decoding / re-cipher processing of digital contents and management of an encryption key / possible ].

[0036]Although such composition is trustworthy when the system configuration lacks in pliability and change of user side equipment or a change of a digital contents control program is made it is serious that a user deals with these change.

[0037]Even if it is a case where change of user side equipment or a change of a digital contents control program is made In order to cope with it flexibly it is desirable for a digital contents control program to be software but change may be performed when a digital contents control program is an application program. Therefore in order for a digital contents control program to be software it is necessary to build a digital contents control program into the kernel which is a fixed area of the operating system (OS) with which a user cannot change.

[0038]However it is not realistic when a digital contents control program is built into a fixed area called a kernel and the digital -contents managerial system and the ciphering system change with databases.

[0039]By there being a thing in which interrupt operation is possible in a real time operating system in real-time slice time earlier figures double [ 1- ] than the time slice time of the system in other operating systems also including a kernel field and using this art as stated above When the Assessment on Search Report by Designated Searching Authority of digital contents with a copyright opinion is supervised and an illegal use is discovered without affecting the whole operation warning or the compulsive stop of use can be carried out. Next how to reinforce a digital contents control program using a real time operating system is explained.

[0040]Since the illegal use of digital contents is performed by [ of the decoded digital contents ] unauthorized processing unauthorized preservation unauthorized copying or unauthorized transmitting the existence of an illegal use is detectable by the existence of processing of decryption digital contents preservation a copy or transmission. Therefore the process of supervising an illegal use interrupts the process which a digital contents control program is performing with a certain time interval and interrupts by multitasking of the preemptive method which supervises compulsorily.

[0041]The multitasking time slice by which normal use is carried out is 10 ms and decoding / re-code process is also performed by this time basis. On the other

handthe fastest real-time slice is 1/100 of 100 microseconds. Thereforeby supervising whether the decoded digital contents have processedsavedcopied or uploaded by the high surveillance task of interrupt prioritiesWhen the Assessment on Search Report by Designated Searching Authority of digital contents with a copyright opinion can be supervised without affecting the just use which the user is performing and an illegal use is discoveredwarning or the compulsive stop of use can be carried out.

[0042]The digital contents control program which has such a monitoring function is built into the subsystem field which operates by not a kernel portion but the user mode of an operating systemand let a supervisory process be a high process of a priority.

[0043]By this compositionthe surveillance of the existence of use of the digital contents in decoding / re-code and the illegal use besides permission can be performed that it is simultaneous and smoothly.

[0044]The composition of the operating system with which the digital contents control program was incorporated is shown in drawing 1. The Management Department (Executive) which operates by the kernel mode in which a user cannot operate this operating systemIt consists of a subsystem which operates by the user mode which a user can operateThe Management Department and a subsystem have interfaced by system service API (Application Programming Interface)HAL (Hardware abstraction Layer) intervenes between hardware and a kernel part.

[0045]The subsystem comprises the central subsystem and application programs which perform the emulation of other operating systemsand screen drawingsuch as an environmental subsystem and a security subsystem.

[0046]The virtual-memory-management function which is the microkernel (micro kernel) at the Management Department (virtual memory manager)An object manageran LPC (Local Procedure Call) functiona process managerand a security reference monitorTo the I/O controlling function (I/O manager) who manages input and output between the kerneldiskand network which are the most fundamental elements. The digital contents control program which manages the digital contents which the copyright opinion was furthermore madei.e.a digital-contents controlling function(digital content manager) is incorporated.

Management of the preservation which is an important portion in management of digital contentsa copyor transmission is performed when a digital-contents controlling function manages an I/O controlling function.

[0047]Working example of the digital-contents managerial system with which the invention in this application is applied was shown in drawing 2. In this digital-contents managerial systemthe surveillance of the digital-contents Assessment on Search Report by Designated Searching Authority by a user is performed via a network. In this figureas for 1a digital-contents control center and 4 are users a database and 2and the user 4the database 1and the digital-contents control center 2 are connected in the network 3 which is a public network or a bidirection

CATV circuit.

[0048] Digital contents are accumulated in the database 1 and encryption digital contents are transmitted to the user 4 via the course 5 shown with the dashed line. The database 1 transmits the encryption key for decoding for carrying out decoding / re-code of the encryption digital contents and the encryption key for re-codes to the digital-contents control center 2 according to the course 6. The digital-contents control center 2 enciphers the encryption key for decoding and the encryption key for re-codes which were transmitted and delivers them to the user 4 via the course shown with the dashed line 7. The digital-contents control center 2 transmits a monitoring program to the user 4 in the course 8 shown as the solid line.

[0049] Although the contents of a utilization permission are managed by the digital contents control program built into the device which the user 4 uses, a possibility that use besides the range which the digital contents control program has managed will be performed by the malicious user cannot be denied thoroughly. The digital contents control program has managed input and output of the user's 4 device. All input and output from the memory in a user, i.e. preservation, a copy and transmission are managed by the digital contents control program and when digital contents are saved, copied and transmitted, they are re-enciphered. However, it is detected by the monitoring program which interrupts a digital contents control program that preservation, copy and transmission of digital contents should be performed by the malicious user even when keeping this management from being possible.

[0050] Monitoring operation is performed by linking a monitoring program with the digital contents control program built into the device which the user 4 uses and interrupting processing of a digital contents control program. It is supervised whether the user is performing use beyond the contents of a utilization permission. The monitoring program which detected that preservation, copy and transmission which is such irregular use were performed is replaced with the display of the warning shown in JPH7-271865A. Embedding of visible digital watermarking shown in drawing 3 (b) to the original digital contents shown in the compulsive re-encryption or drawing 3 (a) by the encryption key with which the stop of decoding processing and a user are not concerned or embedding to the digital contents of invisible digital watermarking shown in drawing 4 (b) is performed.

[0051] The contents of a utilization permission point out here the preservation to simple use of digital contents and built-in memory storage, the copy to an external medium and transmission to other users who go via a network, being embedded as visible digital watermarking -- discernments such as a user's name -- an easy thing is suitable.

[0052] The monitoring program has collaborated during operation of the digital contents control program built in the user's unit. If it has not collaborated with a monitoring program, the digital contents control program is kept from in other words operating. For that purpose, [ whether it makes for the monitoring program to have

started via a network into the conditions for starting a digital contents control programand ] Or if a digital contents control program is startedhe is trying to be automatically started in a monitoring program via a network. When a user uses the digital contents transmitted to a user via a networkit mixes in the digital contents transmitted and a monitoring program is also transmitted.

[0053]A monitoring program is united with a digital contents control programthe monitor command which makes monitoring operation perform to a digital contents control program is transmittedand monitoring operation can be made to perform to a digital contents control program.

[0054]In the digital-contents managerial system performed via a networkin treating digital contents with much amount of informationsuch as image datait uses an ISDN (Integrated System for Digital Network) circuit as a communication line in many cases. What is generally used as this ISDN circuitThe DCH whose data transmission rate called B channel is 64K bps Two channelsAlthough the control channel whose data transmission rate called D channel is 16K bps is transmitted by the DCH of 1-2 channels as those with one channeland a matter of course as for digital contentsD channel is not used in many cases. then -- if it is made like [ performing the interruption surveillance by a monitoring program by this D channel ] -- use of digital contents -- completely -- influence \*\*\*\*\* -- there are nothings and it becomes possible to perform the remote monitor of Assessment on Search Report by Designated Searching Authority.

[0055]By using for download the ADSL (asymmetric digital subscriber line) art in which the data transmission rate of a maximum of 56K bps is realizablen using a public networkThe interruption surveillance by a monitoring program can be performed efficiently.

[0056]What is shown in drawing 4 is an example which embeds digital watermarkingeven if it is a case of regular preservationcopyand transmission included in the contents of a utilization permission. Digital watermarking in this case is invisible digital watermarking detected by a digital-watermarking detection means as shown in (b)and when not based on a digital-watermarking detection meansas it was shown in (a)there is instead of [ no ] apparently with original digital contents. being embedded like the case of visible digital watermarking -- discernmentsuch as a user's name-- an easy thing is suitable.

[0057]By doing in this wayeven if it is regular use in the beginningwhen an illegal use is performed laterthe course of preservationa copyand transmission can be checked. Even if regularby repeating preservationa copyand transmissionas shown in (c)invisible digital watermarking increasesandas a resultthe quality of digital contents deteriorates. According to such a thingit is lost that preservationa copyand transmission are repeated infinitelyand management of digital contents becomes easy.

[0058]"Re-encryption" which is an element important for digital-contents management is the process that a burden is quite heavy for a user's device. Thereforeit is also effective in preventing the illegal use of digital contents to embed digital watermarking as a short form.

[0059]If a user is made for a utilization permission key to come to hand beforehand as shown in JPH7-271865A when use of digital contents is performed for payfee collection will be performed easilybut. When a digital-contents control center charges later the meter ring data which is a use track record by polling recoveringmeter ring data is put under a user's management until polling is performed. Thereforethe alteration of meter ring data is performed by the malicious userand it is possible that normal fee collection is barred.

[0060]When the user uses digital contents in the digital-contents managerial system of this working examplea user's unit is always connected to a control centerand the surveillance of the Assessment on Search Report by Designated Searching Authority by a monitoring program is performed. Thereforeby keeping meter ring data to a digital-contents control center in this monitoring operationthe necessity for polling is lost and the alteration of the meter ring data by a user can be prevented. Even if it is a case where use of digital contents is performed for nothingthe Assessment on Search Report by Designated Searching Authority by a user can be grasped easily.

[0061]The lineblock diagram of other working example of the digital-contents managerial system with which the invention in this application is applied was shown in drawing 5. In this digital-contents managerial systemthe surveillance of digital-contents Assessment on Search Report by Designated Searching Authority is performed by broadcast. In this figureas for 11a digital-contents control center and 14 are users a database and 12and the user 14the database 1and the digital-contents control center 12 are connected in the network 13 which is a public network or a bidirection CATV circuit.

[0062]Digital contents are accumulated in the database 11 and encryption digital contents are transmitted to the user 14 via the course 15 shown with the dashed line. The digital-contents control center 12 enciphers the encryption key for decoding for carrying out decoding / re-code of the encryption digital contentsand the encryption key for re-codesand delivers them to the user 14 via the course shown with the dashed line 17. The digital-contents control center 12 transmits a monitor command to the broadcasting station 19and the broadcasting station 19 transmits the transmitted monitor command to the user 14 in the course 18 shown as the solid line.

[0063]Although this course 18 has the most common broadcasting electric-wave the CATV cables which are cable broadcasting are also availableand it is also possible to use a network when Internet broadcasting is performed further.

[0064]This monitor command interrupts the operation which the digital contents control program built into the device which the user 14 uses is performingA user makes a digital contents control program supervise whether use beyond the contents of a utilization permission is performedInvisible digital watermarking shown in visible digital watermarking which made suspend decoding processing when preservationcopyand transmission were performedor was shown in drawing 3or drawing 4 is embedded at digital contents.

[0065]The monitor command is performing interrupt operation during operation of



the digital contents control program built in the user's unit. If the broadcast wave it is broadcast that a monitor command is not received the digital contents control program is kept from in other words operating. For that purpose if it makes to have received the monitor command via a broadcast wave into the conditions for starting a digital contents control program or a digital contents control program is started the monitor command which goes via a broadcast wave automatically will be received. When a user uses the digital contents transmitted to a user by data broadcasting etc. it mixes in the digital contents transmitted and a monitor command is also transmitted.

[0066] The digital contents control program has managed input and output of the user's 14 device. All input and output from the memory in a user's e.g. preservation copy and transmission are managed by a digital contents control program and when digital contents are saved, copied and transmitted they are re-enciphered. It is detected by the monitoring program which interrupts a digital contents control program that preservation copy and transmission of digital contents should be performed by the malicious user even when keeping this management from being possible.

[0067] The monitoring program which detected that such irregular use was performed is replaced with the display of the warning shown in JPH7-271865A and embedding of visible digital watermarking as shown in drawing 3 (b) is performed. Even if it is a case of regular preservation copy and transmission included in the contents of a utilization permission it is also possible to embed invisible digital watermarking which will not be detected without a digital-watermarking detection means as shown in drawing 4 (b) and (c).

[0068] A user does not perform monitoring operation through these broadcasts or networks of a user's volition but when using the digital contents which the copyright opinion was made it is automatically performed by the digital contents control program. In order to ensure this operation furthermore when monitoring operation through broadcast or a network is not performed it is made by not performing operation of decoding/encryption by a digital contents control program. When using the digital contents which the copyright opinion was made it is automatically connected to the control center which transmits the reception or the monitoring program of an electric wave which broadcasts a monitoring program.

[0069] Next working example which distributes a public key is described. As opposed to it being about 100 bits which has a large size of the encryption key used by the secret key (secret key) system called a common key (common key) system. What has a large encryption key used by a public key (public key) system exceeds 1000 bits. Since a public key system requires time and effort for encryption/decryption while safety is high it is used for a data encryption with small sending of a secret key, digital signature and amount of attestation isochore and encryption of digital contents is performed using a secret key. Although a public key and a specified key (private key) can be put together and cannot be used and others cannot be known for a public key system under an owner's management as for a specified key the public key needs to be told to

others on the purpose of use.

[0070]Therefore although there are few possibilities that a fake public key may be distributed if a public key can be directly received from an owner in that case although a public key is distributed to the public by various means when that is not right a fake public key may be received. the digital-contents managerial system which can look like [ business ] the truth of the public key distributed also in the indirect distribution method of going via broadcast or a network in the public key in this working example and can check it -- so to speak a key distribution network is proposed.

[0071]Working example of this invention of the digital-contents managerial system which distributes a public key by broadcast is shown in drawing 6. In this digital-contents managerial system since it is generally delivered widely a public key can be used as a simple authentication method replaced with the PEM (Privacy Enhanced Mail) method adopted with the public key authentic method in Electronic Commerce Technology Division etc.

[0072]As for a public key control center and 23 in this figure 21 is [ a network and 25 ] users a broadcasting station and 24 a public key owner and 22. The broadcasting station 23 A terrestrial analog a satellite analog a CATV analog terrestrial digital It is Television Sub-Division or audio broadcast office such as satellite digital and CATV digital and data broadcasting is performed by proper means such as scanning line multiplex (Vertical Blanking Interval: VBI) voice multiplex and data mixing. An Internet broadcasting office is also available as this broadcasting station. The network 24 is a public network or a bidirection CATV circuit and it is connected in the network 24 between the public key control center 22 and the user 25 and is connected by the proper information transmission medium between the broadcasting station 23 and the user 25.

[0073]the public key and public key owner whom the public key owner 21 owns in the digital-contents managerial system constituted in this way -- it transmits to the public key control center 22 according to the course 26 by using a certain data proving being the person himself/herself as the data for public key owner discernment. Although information including a public key owner name etc. is directly used as data for public key owner discernment used here the electronic fingerprints which reduced the information to 16 bytes of data by the MD5 hash algorithm can also be used.

[0074]The public key control center prepares the public key distribution screen as shown in drawing 7 (a) and inserts a public key in a position. This screen is created using HTML (Hyper Text Markup Language) form or XML (eXtensible Markup Language) form so that the inserted public key can be used dissociating easily. The image data is inserted in the part.

[0075]At this image data the public key owner's 21 data for discernment (OWNER'S ID) is embedded as invisible digital watermarking. Only the public key control center knows this invisible algorithm and embedding position of digital watermarking as the public key control center was shown in drawing 7 (b) can know the contents of digital watermarking but. When other persons see it is a usual

screen like drawing 7 (a) and the contents of digital watermarking cannot be known. [0076] If the advertisement is published as this image screen, the cost which public key distribution takes can be covered by the charge of advertising printing. Into other portions, additional information such as emergency intelligence and announcement information can be published. A time stamp may be added in order to manage providing a shelf-life etc. Although it is optimal to use a photograph as this image data, when voice data is available, it is also possible to embed digital watermarking at the voice data used.

[0077] The broadcasting station 23 broadcasts the public key distribution screen which did in this way and was created according to the broadcast course 28.

[0078] Although the user 25 receives the broadcast public key distribution screen since digital watermarking embedded in the image screen of the public key distribution screen which the user 25 received is an invisible thing, the user 25 cannot know the contents of digital watermarking.

[0079] Although the user 25 separates a public key from the broadcast public key distribution screen and uses it for various Electronic Commerce Technology Division, when it has doubt in the truth of a public key, he transmits a public key distribution screen to the public key control center 22 according to the course 29 by the network 24.

[0080] The public key control center 22 verifies invisible digital watermarking embedded in the image screen of the transmitted public key distribution screen and notifies the user 25 of it according to the course 30 by the network 24 about a public key owner's identification information detected as shown in drawing 7 (b).

[0081] By doing in this way, when others have become completely the \*\*\*\*\* can be detected. In that case, verification becomes very simple when electronic fingerprints are used as a public key owner's identification information.

[0082] It is possible to use the photograph of the person himself/herself for an image screen as the public key owner's intention showed to a favorite screen as shown in drawing 7 (c) or drawing 7 (d) in addition to the advertisement. The charge of printing can be collected in these cases and it can be appropriate for broadcast expense.

[0083] Although it is made for invisible digital watermarking embedded in this working example to have only the public key control center checked, only as for a check, a user can do it. In that case, a user can check electronic fingerprints to a public key owner using electronic fingerprints as public key owner identification information.

[0084] By drawing 8a, a public key describes other working example of this invention distributed according to a user's demand. The digital-contents managerial system which distributes a public key by broadcast explained about drawing 6 is an effective system when distributing a public key mainly to many and unspecified users such as Electronic Commerce Technology Division. On the other hand, when sending individual mail, the partner who distributes a public key is a specific small number in many cases and does not need to distribute by broadcast. In the digital-contents managerial system shown in drawing 8, since it is individually delivered via

a network a public key can be used as a simple authentication method replaced with the PGP (Pretty Good Privacy) method adopted with the public key authentic method in an E-mail etc.

[0085]As for a public key owner and 32 in this figure a network and 34 are users a public key control center and 33 31. The network 33 is a public network or a bidirection CATV circuit. It is connected in the network 33 between the public key owner 31 and the user 34 and between the public key control center 32 and the user 34 and is connected by a proper information transmission means between the public key owner 31 and the public key control center 32.

[0086]as the public key and the data for public key owner discernment which the public key owner 31 owns in the digital-contents managerial system constituted in this way -- a public key owner -- a certain data proving being the person himself/herself is transmitted to the public key control center 32 according to the course 35 which goes via the network 33.

[0087]The public key control center 32 embeds public key owner identification data as invisible digital watermarking in the image screen of a public key distribution screen while inserting a public key in the position of the public key distribution screen shown in drawing 7 (a) and it returns it to the public key owner 31 according to the course 36. Since the data for public key owner discernment and the public key distribution screen which are used also in this digital-contents managerial system are the same as that of the case of the digital-contents managerial system shown in drawing 6 explanation here for the second time is omitted.

[0088]The user 34 who is going to obtain the public key owner's 31 public key requests distribution of a public key from the public key owner 31 according to the course 37 via the network 33 and the public key owner 31 transmits a public key distribution screen to the user 34 according to the course 38 which goes via the network 33 according to this request.

[0089]The user 34 separates a public key from the transmitted public key distribution screen and enciphers an E-mail using the separated public key and transmits to the public key owner 31. The public key owner 31 decodes using the specified key which owns an encrypted mail.

[0090]When the user 34 has doubt in the truth of the transmitted public key the public key distribution screen transmitted by the course 39 is transmitted to the public key control center 32. The public key control center 32 verifies invisible digital watermarking embedded in the image screen of the transmitted public key distribution screen and notifies the user 34 of the result according to the course 40. By doing in this way when others have become the public key owner 31 completely the \*\*\*\*\* can be detected.

[0091]It can also constitute from this working example although the public key owner 31 has distributed the public key distribution screen to the user 34 directly in addition so that the public key control center 32 may manage and distribute a public key distribution screen.

[0092]By drawing 9 and drawing 10a a public key describes working example of

further others of this invention distributed according to a user's demand. In this working example the public key for Electronic Commerce Technology Division is dealt with. Although the public key owner is verified using digital watermarking in working example shown in working example shown in drawing 6 and drawing 8a public key user is verified in working example shown in drawing 9 and drawing 10. [0093] As for a public key owner and 42 in the digital-contents managerial system shown in drawing 9a network and 44 are users a public key control center and 43 41. The network 43 is a public network or a bidirection CATV circuit and is respectively connected by the network 43 between the user 44 and the public key control center 42 between the public key owner 41 and the public key control center 42 between the public key owner 41 and the user 44.

[0094] In the digital-contents managerial system constituted in this way first the public key owner 41 transmits the public key to own to the public key control center 42 according to the course 45 and the public key control center 42 is keeping the transmitted public key. The user 44 who tries to perform acts such as order by Electronic Commerce Technology Division to the public key owner 41 transmits a certain user-identification data proving the user's 44 identity to the public key control center 42 according to the course 46 which goes via the network 43.

[0095] The public key control center 42 embeds the user's 44 identification data as invisible digital watermarking in the image screen of a public key distribution screen as it was shown in drawing 10 (b) while inserting the public key in the predetermined public key insertion point of the public key distribution screen shown in drawing 10 (a). It transmits to the user 44 according to the course 47 which goes via the network 43.

[0096] Although it is also possible to use information including a user name etc. directly as data for user identifications used here the electronic fingerprints which reduced the information to 16 bytes of data by the MD5 hash algorithm can be used.

[0097] The public key distribution screen is created using HTML form or XML form so that the inserted public key can be separated easily and the image data is inserted in the part. At this image data the user's 44 identification data (USER'S ID) is embedded as invisible digital watermarking. Only the public key control center knows this invisible algorithm and embedding position of digital watermarking when a public key control center checks can know the contents like to drawing 10 (b) but. When other persons see it is a usual screen like drawing 10 (a) and the contents of digital watermarking cannot be known.

[0098] This image screen can cover the cost which public key distribution takes by an advertising rate if the advertisement is used. Into other portions additional informations such as emergency intelligence and announcement information can be published. A time stamp may be added in order to manage providing a shelf-life etc. Although it is optimal to use a photograph as for this image data when voice data is available it is also possible to embed digital watermarking at the voice data used.

[0099] The user 44 separates a public key from the transmitted public key

distribution screen and using the separated public key it enciphers and he transmits a purchase order to the public key owner 41 with the transmitted public key distribution screen. The public key owner 41 decodes using the specified key which owns an encryption purchase order and performs ordering business.

[0100] When the public key owner 41 has doubt in the truth of a purchaser the public key distribution screen transmitted by the course 48 which goes via the network 43 is transmitted to the public key control center 42. The public key control center 42 verifies invisible digital watermarking embedded in the image screen of the transmitted public key distribution screen and notifies the public key owner 41 of the result according to the course 49. The \*\*\*\*\* can be detected when others have become the user 44 completely by doing in this way.

[0101] It is possible to use the photograph of the person himself/herself for an image screen as the public key owner's intention showed to a favorite screen as shown in drawing 10 (c) or drawing 10 (d) in addition to the advertisement. The charge of printing can be collected in these cases and it can appropriate for broadcast expense.

---

## DESCRIPTION OF DRAWINGS

---

[Brief Description of the Drawings]

[Drawing 1] The construct figure of the operating system with a digital-contents controlling function used by this invention.

[Drawing 2] The lineblock diagram of the digital data managerial system of this invention which performs the illegal use surveillance of digital contents.

[Drawing 3] The explanatory view of the controlled state by the digital data managerial system of this invention.

[Drawing 4] The explanatory view of other controlled states by the digital data managerial system of this invention.

[Drawing 5] The lineblock diagram of other digital data managerial systems of this invention which performs the illegal use surveillance of digital contents.

[Drawing 6] The lineblock diagram of the digital data managerial system of this invention which distributes the public key used in order to manage digital contents.

[Drawing 7] The explanatory view of the method of distributing the public key by the digital data managerial system of drawing 6.

[Drawing 8] The lineblock diagram of other digital data managerial systems of this invention which distributes the public key used in order to manage digital contents.

[Drawing 9] The lineblock diagram of the digital data managerial system of further others of this invention which distributes the public key used in order to manage digital contents.

[Drawing 10] The explanatory view of the method of distributing the public key by the digital data managerial system of drawing 9.

[Description of Notations]

1 Database



2 Digital-contents control center  
3132433and 43 Network  
4142534and 44 User  
11 Database  
12 Digital-contents control center  
19 and 23 Broadcasting station  
2131and 41 Public key owner  
2232and 42 Public key control center

---